

REMARKS

The currently pending claims 29 and 30 have been rejected over Marvit in view of Burrows. Applicants respectfully traverse and beg for reconsideration in view of the remarks that follow.

The present invention

A protocol according to the present invention involves three actors: Network A, Network B, and mobile station M. A typical scenario using this protocol plays out as follows:

M contacts B and requests to have a session with it. B demands that M authenticate itself before B will communicate with it. Even though M has given B its identification number (IMSI), B is not satisfied. The identification number has not yet been authenticated.

Mobile station M has established with Network A a key (K) for encrypting communications between M and A. Network B has a secure line through which it can communicate with Network A.

Network B now generates an authentication key (SSD) which is to be used by M for generating a message that will authenticate M to network B.

Network B is facing two problems: (1) It must deliver SSD to mobile station M despite the fact that Network B is not yet willing to communicate directly with M; and (2) It must have assurance that the mobile station to which SSD is delivered really is M and not some impostor.

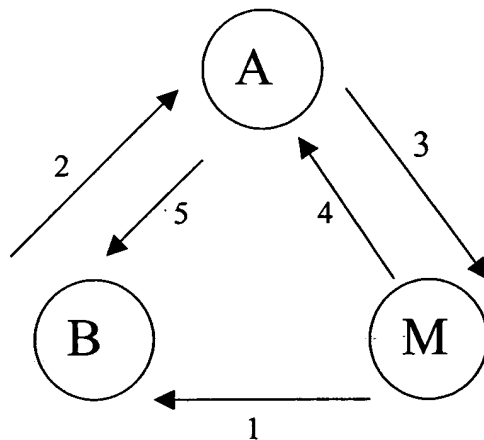
The present invention provides a protocol that solves both problems. It is assumed that M has already authenticated itself to Network A. (This would typically have to occur before key K could be established for encrypting communications between M and A.) Therefore, both problems are solved by having SSD delivered in two stages. First, B delivers SSD to A over the secure line. Then, A protects SSD by encrypting it with K, and delivers it in encrypted form to M.

As soon as SSD is delivered to M, M can authenticate itself to B. M generates an authentication signal by combining SSD with IMSI (e.g., by using SSD as a key for encrypting IMSI). M sends the authentication signal to A, and A forwards it to B. B can compare the received signal with a locally generated counterpart. If the signals match, B can consent to a session with M.

Thus, one important feature of the invention is that Network A forwards the authentication key (SSD) from B to M. This provides enhanced security because Network A already “knows” the mobile station that claims to be M and has established a secure channel for communicating with it.

In the terminology and notation used by M. Burrows et al., “A Logic of Authentication,” a protocol according to the present invention may be summarized as follows. We assume that the key K has already been exchanged between mobile station M and Network A.

Message 1	$M \rightarrow B : \text{IMSI}$	The mobile identifies itself to B and requests a session.
Message 2	$B \rightarrow A : \text{SSD}$	B sends the authentication key to A over a secure line
Message 3	$A \rightarrow M : \{\text{SSD}\}_K$	A encrypts the authentication key and sends it to M
Message 4	$M \rightarrow A : \langle M \rangle_{\text{SSD}}$	M generates authentication signature, sends it to A
Message 5	$A \rightarrow B : \langle M \rangle_{\text{SSD}}$	A forwards authentication signature to B



The protocol described by Burrows at page 18

The Needham-Schroeder Protocol which Burrows describes on page 18 addresses a different problem. There, entity A and entity B wish to establish a session key K_{ab} for talking to each other. The key is provided by server S. Server S knows two more keys: key K_{as} known only to A and S, and key K_{bs} known only to B and S.

However, only entity A communicates directly with server S. Therefore, S is faced with this problem: How to safely deliver K_{ab} to B before secure communications are established between A and B.

According to the solution which Burrows describes, S sends K_{ab} to A under the protection of K_{as} . Also under the protection of K_{as} , S sends a message to A for forwarding to B. Before sending that message, S encrypts it using K_{bs} , so A cannot access it or alter it, and eavesdroppers cannot access it. That message contains the session key K_{ab} , but in a form that is accessible only to B.

Differences between Burrows, page 18, and the present invention

1. Burrows is for key distribution, whereas the present invention is for authentication.

The motivation in Burrows is to have S provide a key for a session between A and B. S must distribute the key to both A and B. S must give the key to A for forwarding to B, while preventing A from tampering with the key before forwarding it and preventing eavesdroppers from accessing it.

By contrast, the motivation for the present invention is to have a wireless station M authenticate itself to a wireless network B before a session between B and M can begin. M can communicate only over the air. M cannot communicate directly with B until it has authenticated itself.

The result in Burrows is that A receives the session key from S directly, B receives the session key from S via A, and a session can begin between A and B.

By contrast, the result according to Applicants' claim 1 is that M receives the authentication key from B via network A, and B receives M's response via

network A. Encryption with the key K assures that the over-the-air transmissions from A to M and from M to A are secure.

Thus, the present invention differs both in motivation and result from Burrows.

2. Burrows does not suggest taking advantage of security features of wireless networks.

Among other things, it will be seen that Burrows does not suggest using a second wireless network (A) to facilitate secure communications between a mobile station (M) and a first wireless network (B). In particular, Burrows fails to suggest using established, or readily established, security measures such as encryption key K between the mobile station and network A to assure that over-the-air communications to and from the mobile station will be secure.

3. The roles of the respective actors in the Burrows protocol are distinctly different from those in the claimed protocol.

Moreover, the roles of the respective parties in Burrows are different from the roles of the respective parties according to the present invention. The objective in both Burrows and the present invention is, arguably, to facilitate a "session" between two parties, which are A and B in Burrows, and M and B in Applicants' claim 1.

In both cases, there is a "third party" that does not participate directly in the session. The Burrows protocol involves S as such a "third party" and the present claim 1 involves A as a third party.

In Burrows, the information to be distributed originates with the third party S, and is forwarded by one of the parties to the session (i.e., by party A). By contrast, Applicants' invention has the information to be distributed originate with one of the parties to the session (i.e., SSD originates with B, authentication signature originates with M), and has that information forwarded by the third party (i.e., by network A).

4. The Burrows forwarding function and the inventive forwarding function serve different purposes.

Furthermore, Applicants' protocol involves two communications forwarded in opposite directions by network A prior to establishment of the "session," whereas Burrows only has its party A forwarding in one direction to B.

The protocol described at Burrows, page 25

The protocol at Burrows, page 25, is for A to send a session key to B via S, with security provided by encryption under one key shared by A and S, and under a second key shared by B and S. The discussion at Burrows, page 25, does not suggest the present invention at least for the reasons pointed out above, *mutatis mutandis*, in items 1, 2, and 4.

There is no motivation to combine the teaching at Burrows, page 18, with the teaching at Burrows, page 25, because the respective protocols serve completely different purposes. That is, the protocol at page 18 distributes a key from the third party to both A and B, whereas the protocol at page 25 has A distribute the key to B via the third party.

Marvit teaches away from Burrows, page 18 and Burrows, page 25

To the extent pertinent, Marvit merely describes a key-distribution scheme in which the third party distributes a key to a sender and a key to a receiver. The respective keys need not be the same, but each party needs its respective key in order for a successful communication to take place. Importantly, no forwarding of any kind takes place. Instead, the third party communicates directly with both the sender and the receiver. This is completely contrary to what Burrows teaches at page 18 and page 25.

Thus, there is no motivation to combine Marvit with Burrows, page 18, or with Burrows, page 25.

Marvit fails to suggest the present invention

Marvik deals only with key distribution, not authentication. Marvik does not address any problem in which forwarding is necessary, or in which one party to a session needs to distribute information to the other party to the session. Marvik is silent regarding any security issues specific to wireless communication.

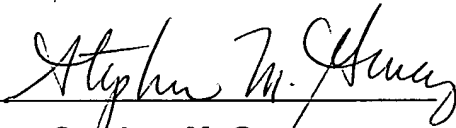
Conclusion

Accordingly, Applicants respectfully submit that singly or in any combination, Burrows page 18, Burrows page 25, and Marvit fail to teach or suggest the claimed invention.

Therefore, withdrawal of the rejection and passage of the claims to allowance is respectfully requested.

Respectfully submitted,

**Douglas N. Knisely
Robert Jerrold Marks
Semyon B. Mizikovsky**

By 
**Stephen M. Gurey
Attorney for the Applicant
Reg. No. 27,336
(973)-386-8252**

Date: May 5, 2005

**Docket Administrator (Room 3J-219)
Lucent Technologies Inc.
101 Crawfords Corner Road
Holmdel, NJ 07733-3030**